Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

General Government & Information Technology Committee

HB 1467

Brief Description: Requiring adoption of data encryption standards for state agencies.

Sponsors: Representatives Hudgins, Stanford, S. Hunt and Ormsby.

Brief Summary of Bill

- Requires the Office of the Chief Information Officer (OCIO) to adopt standards for classifying and encrypting electronic data.
- Requires state agencies to comply with the encryption standards adopted by the OCIO.
- Requires the OCIO to update the encryption standards annually.
- Allows the OCIO to grant a waiver to adopted policies in cases where encryption would be unreasonably costly.

Hearing Date: 1/30/15

Staff: Derek Rutter (786-7157).

Background:

Office of the Chief Information Officer
The Office of the Chief Information Officer (OCIO) was created in 2011 within the Office of Financial Management (OFM). The OCIO is responsible for the preparation and implementation of a strategic information technology (IT) plan and enterprise architecture for the state. The OCIO's duties include standardization and consolidation of IT infrastructure and establishment of IT standards and policies. The OCIO also prepares a biennial state performance report on IT, evaluates current IT spending and budget requests, and oversees major IT projects.

OCIO Data Security Policies

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

The OCIO has established a policy for classifying and securely managing state agency data. According to this policy, agencies must classify data into categories based on the sensitivity of the data. There are four categories defined in the current policy: public information, sensitive information, confidential information, and confidential information requiring special handling. The policy requires the last two categories of data be encrypted using industry standard encryption methods validated by the National Institute of Standards and Technology (NIST). It also defines standards for sharing and transferring data in these categories.

Summary of Bill:

The OCIO must adopt data encryption standards, including a classification schedule for ranking data sensitivity and technical requirements for encryption appropriate to each classification. State agencies must classify all data held on state data networks according to the adopted schedule and comply with the accompanying encryption standards. The standards must include a requirement that the highest sensitivity data be encrypted while at rest on state data systems. The OCIO is directed to update the adopted standards annually, distribute the updates to state information technology directors, and include a phase-in timeline for any new technologies required by the updates. The OCIO may grant waivers to the adopted policies where encryption would be unreasonably costly.

Appropriation: None.

Fiscal Note: Requested.

Effective Date: The bill takes effect 90 days after adjournment of the session in which the bill is passed.